# Configuring HP Integrated Lights-Out 3 with Microsoft Active Directory

HOWTO, 2nd edition

# Introduction

This paper tells you how to integrate HP Integrated Lights-Out 3 (iLO 3) processors with Microsoft® Windows® Active Directory (AD) software to streamline configuration and avoid possible security issues. It describes how to validate the directory after you finish the integration. The rest of this paper refers to iLO 3 simply as iLO.

Integrating iLO with AD lets you have the same level of security as when you log into a Windows environment. Using iLO with AD lets you set up group access to iLO processors. AD passes to iLO a list of groups that contain the authenticated user. iLO compares the AD group list with the iLO database. iLO uses a group match to build a list of authorized privileges for the authenticated user.

There are two LDAP methods for integrating iLO with AD: the HP Extended Schema method and the Default Schema method. This paper describes the Default Schema method (also known as schema-free integration). It is the most convenient way to integrate iLO with AD. It lets you configure the iLO software for two levels of login flexibility:

- Minimum login flexibility requires a fully distinguished name, a password, and membership in a group recognized by iLO.
- Better login flexibility requires a login name combined with user context.

iLO3 v1.20 and later versions also support the Kerberos method for integrating iLO with AD. That method provides a single sign-on.

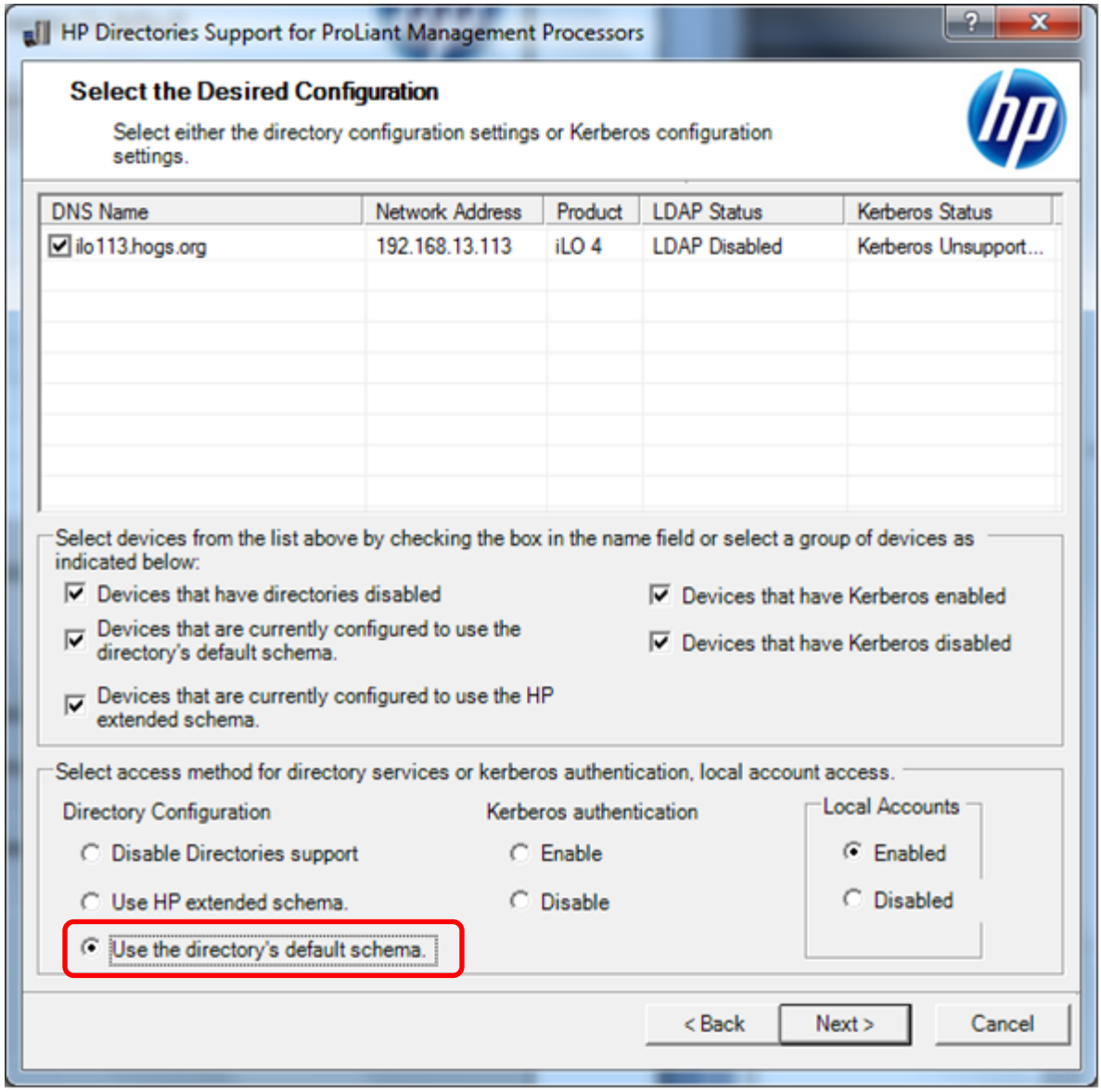
You can do automated schema-free integration using the Lights-Out Migration Utility, manual schema-free integration using the iLO web interface, or automated Kerberos integration using the Kerberos web interface.

# Integration using the Lights-Out Migration Utility

Using the Lights-Out Migration Utility (v2.0 or greater) is the easiest way to set up iLO processors to use AD. Use the following process to set up schema-free integration.

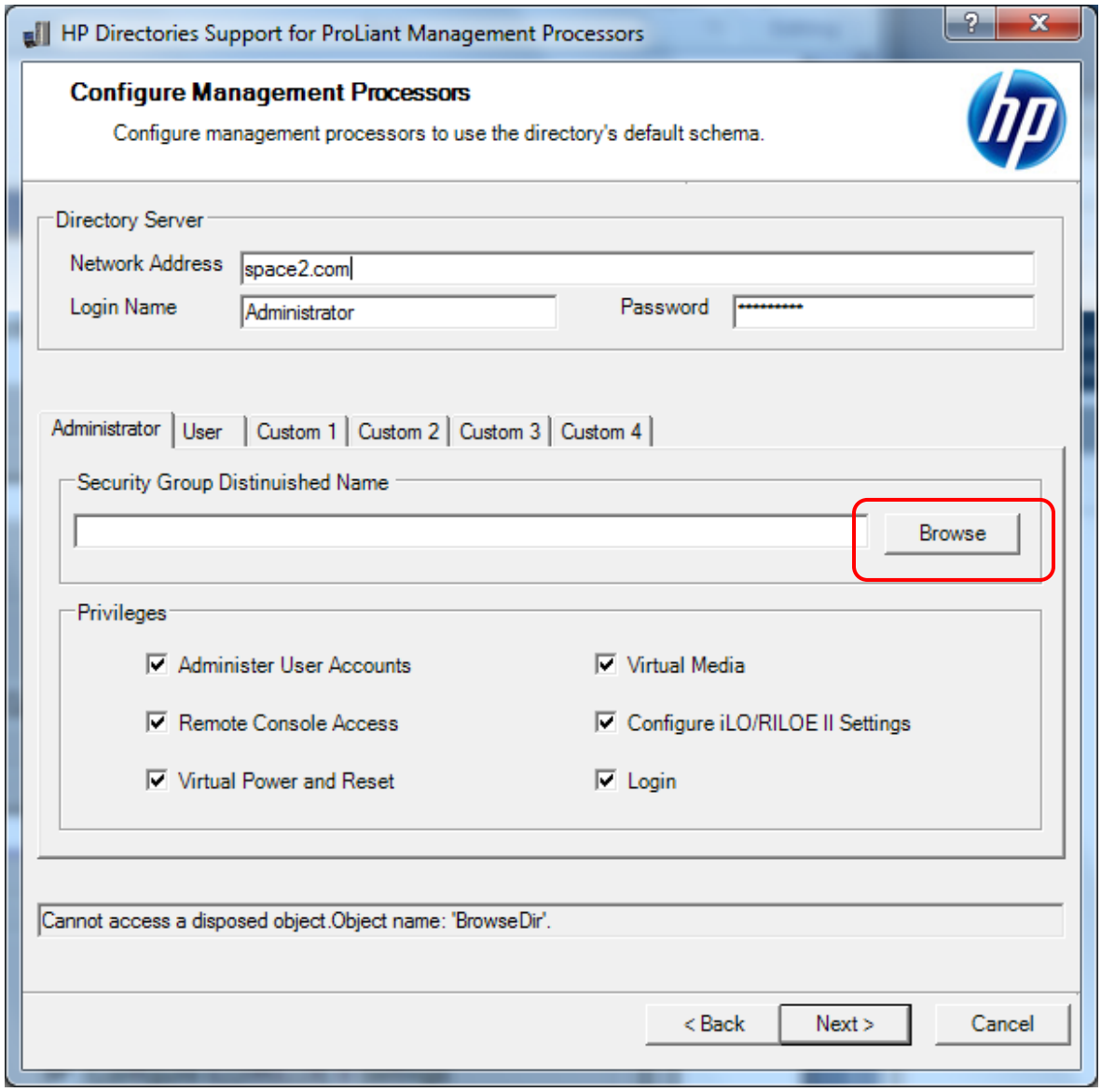
1. Open the HPQLOMIG.EXE utility. Click **Next** at the main screen. The utility will discover the iLO processors and list them in the Select Directory Access Method screen.
2. Select the **Use the directory's default schema** option and click **Next** (Figure 1).

**Figure 1:** HPQLOMIG directory access window lets you select Directory Configuration or Kerberos authentication.



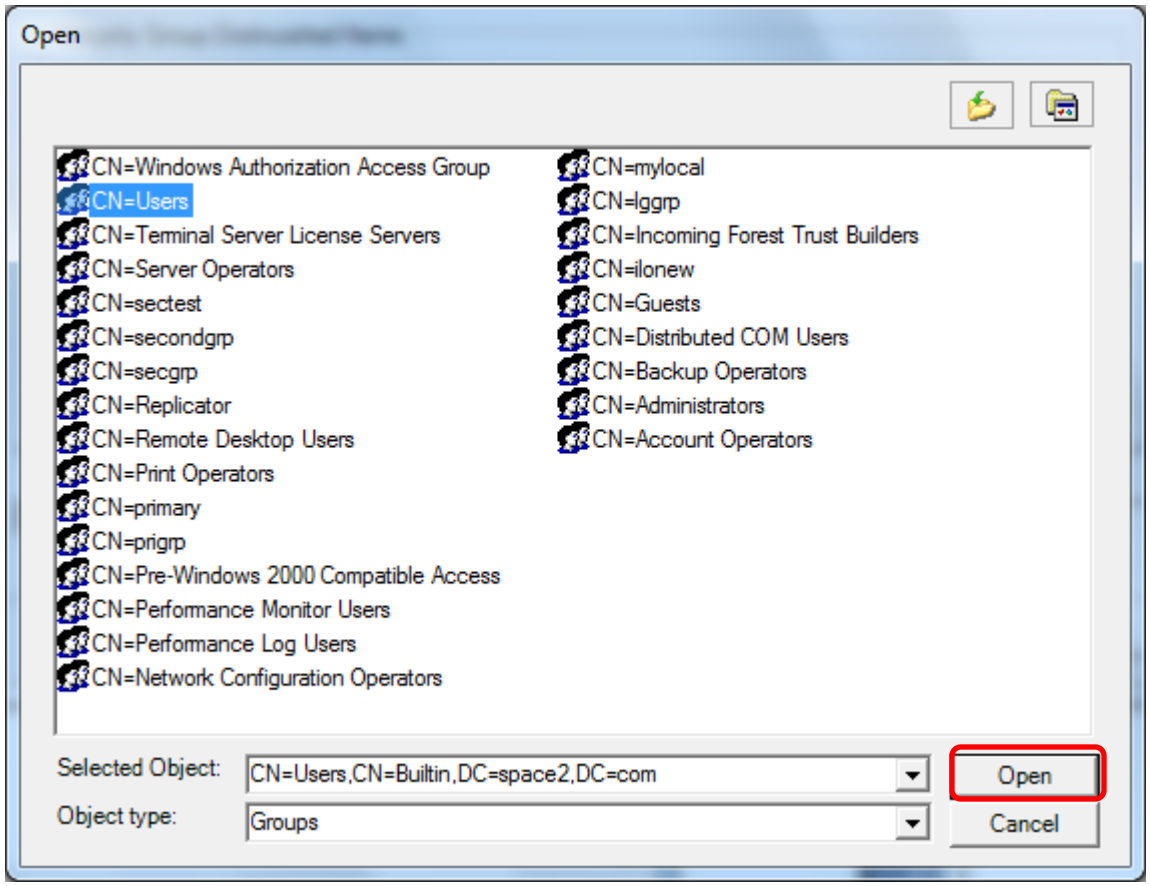
3. Go to the Configure Management Processors window to browse the directory for security groups (Figure 2). Click **Browse** and then **Next**.

**Figure 2:** Use the HPQLOMIG Configure Management Processor window to browse for security groups.



4. A new window opens (Figure 3). Select a group and click **Open**. This step sets privileges for the selected group.

**Figure 3:** Set privileges in the HPQLOMIG distinguished name security groups window.




5. Repeat steps 3 and 4 for each group you want to assign privileges.

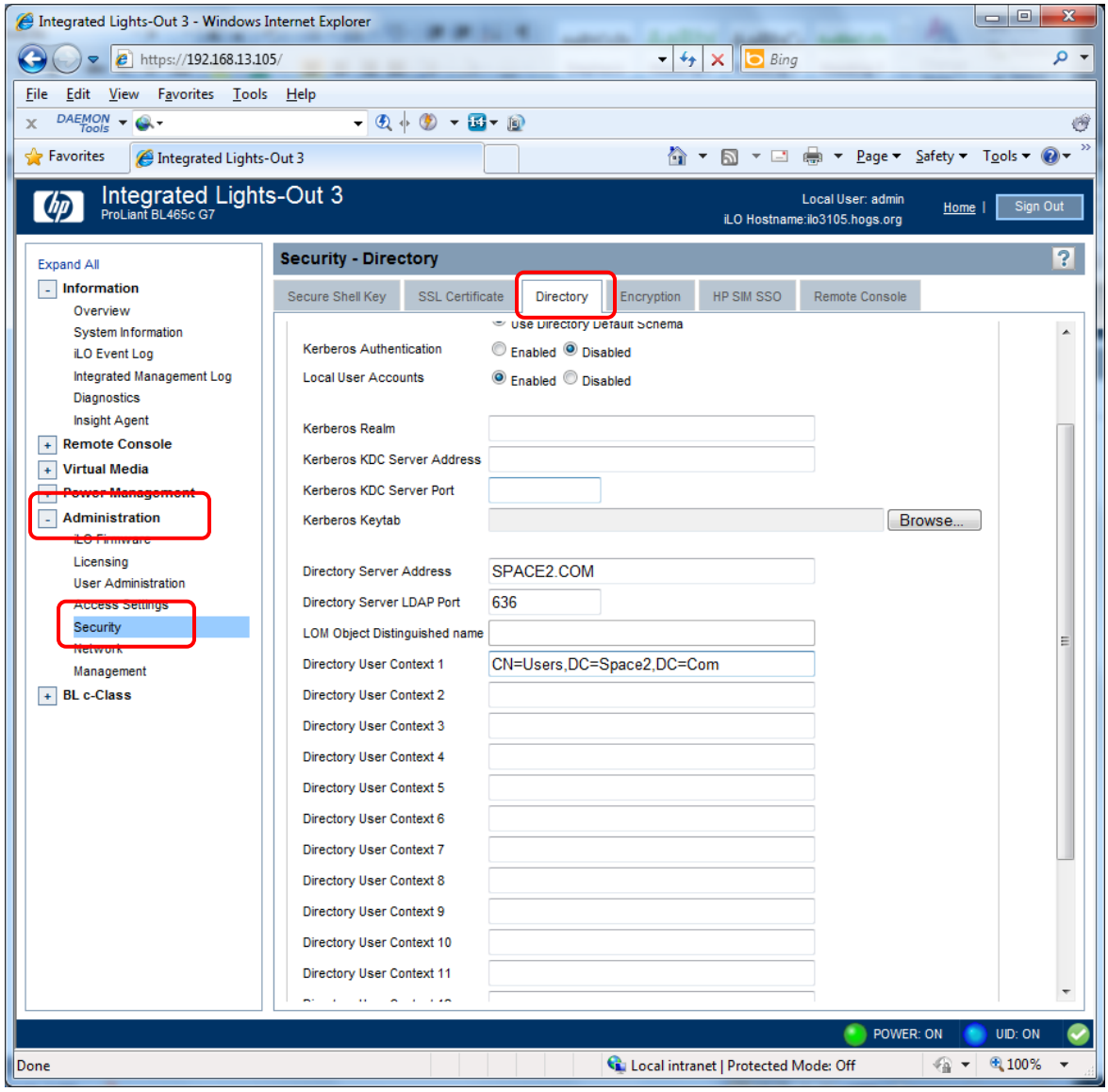
After you set the group privileges, you are ready to validate the directory. Go to the "Validating the directory" section of this paper.

# Integration using the iLO web interface

Complete the following steps to use the iLO web interface to set up schema-free integration with AD.

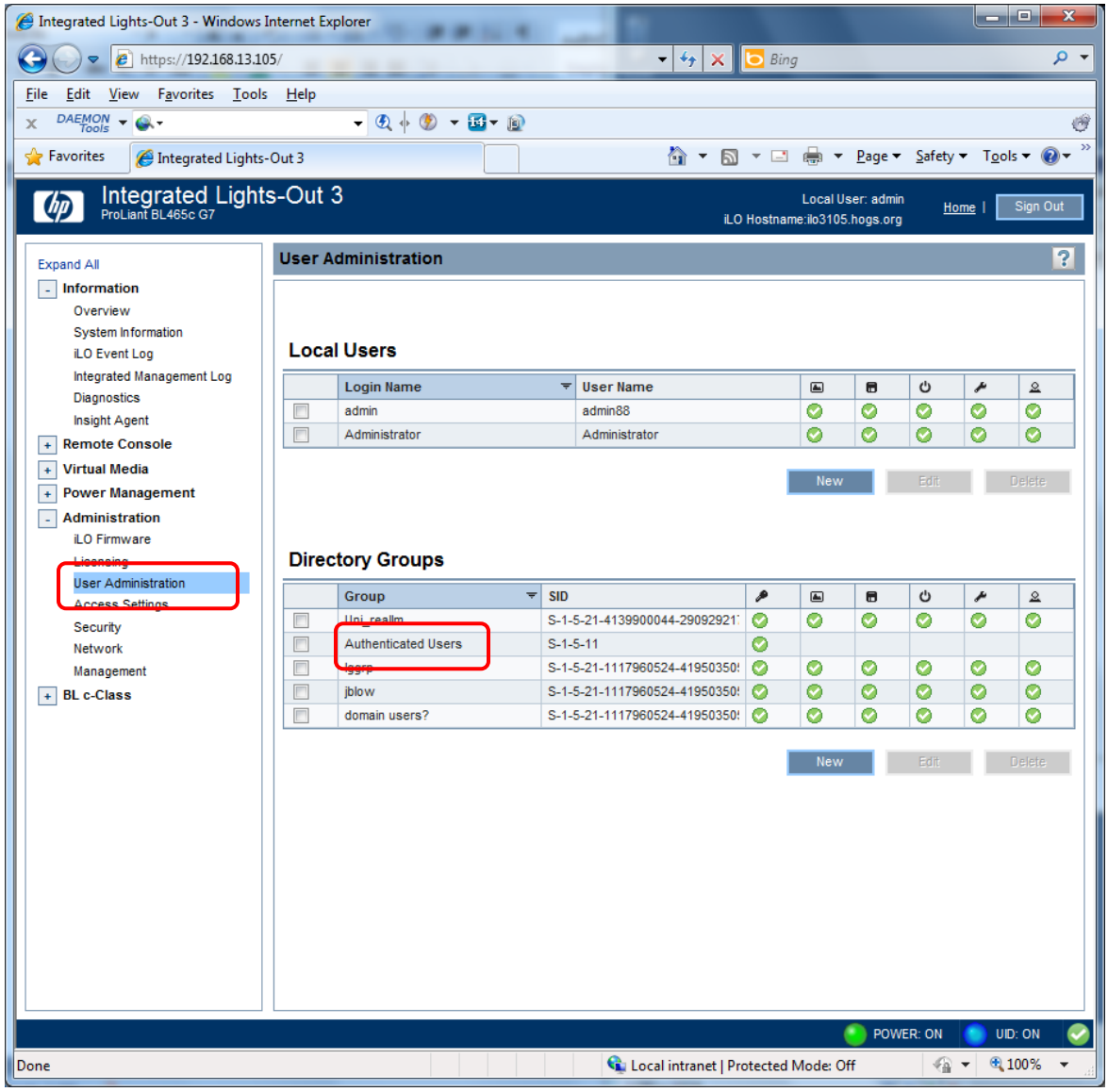
1. Open the iLO software and click on the **Administration** tab (Figure 4):
   a. Highlight Security in the left pane.
   b. Select the **Directory** tab in the Security window.
   c. Select the **Use Directory Default Schema** option and click **Administer Groups**.

**Figure 4:** Use the iLO web interface to set up schema-free integration with AD.



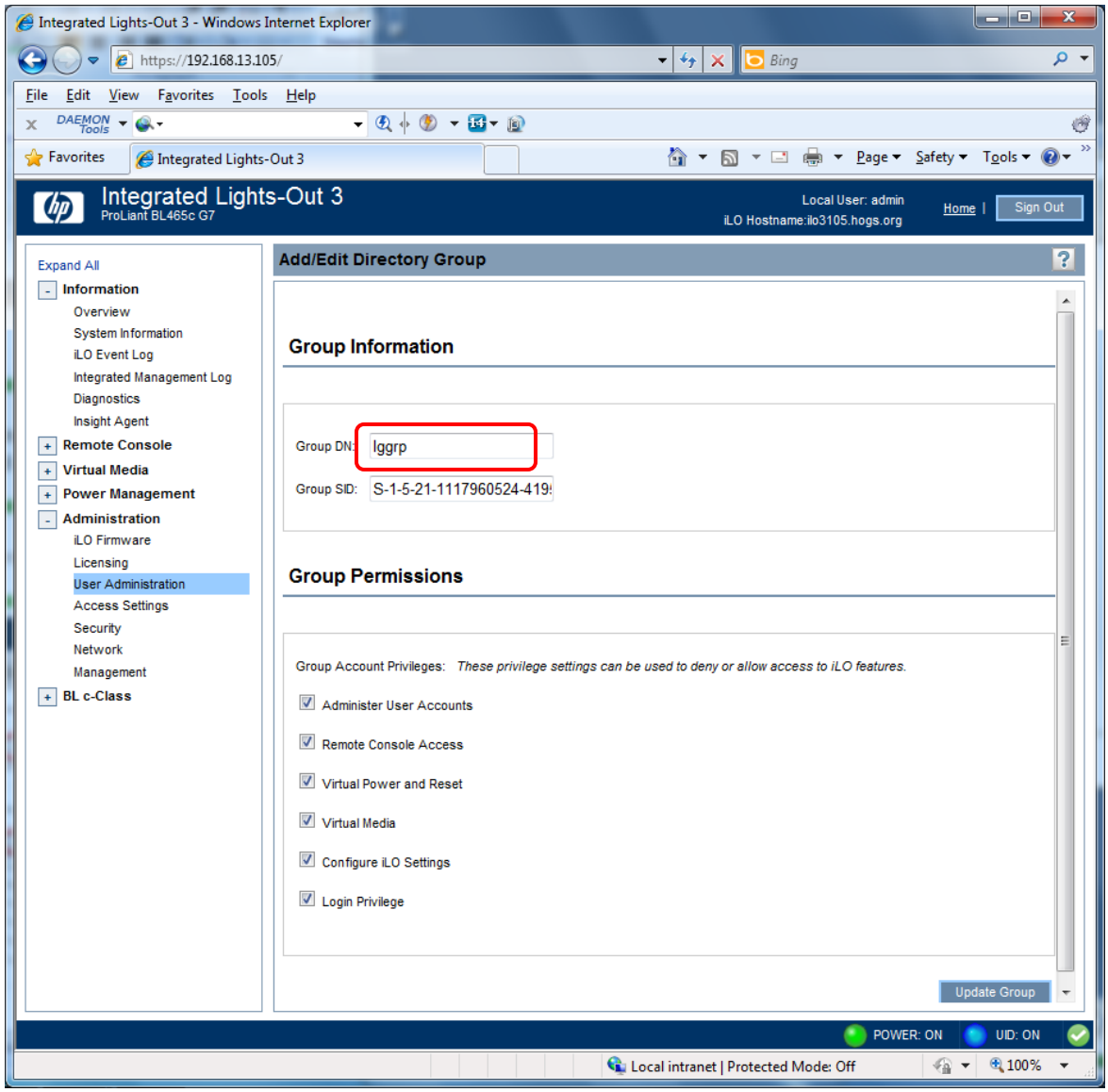
2. In the User Administration window, select the group that you want to modify (Administrator in Figure 5). Click **Edit** or **New** and complete the following step, which is the same for both options.

**Figure 5:** In the User Administration window, select the group you want to modify.



3. Enter the group distinguished name in the Edit Directory Group window. Select the desired group privileges and click **Update Group** (Figure 6).

**Figure 6:** Modify group settings in the Add/Edit Directory Group window.




After you set the group privileges, you are ready to validate the directory. Go to the "Validating the directory" section of this paper.

# Integration using the Kerberos web interface

The following iLO configuration parameters apply to Kerberos login:

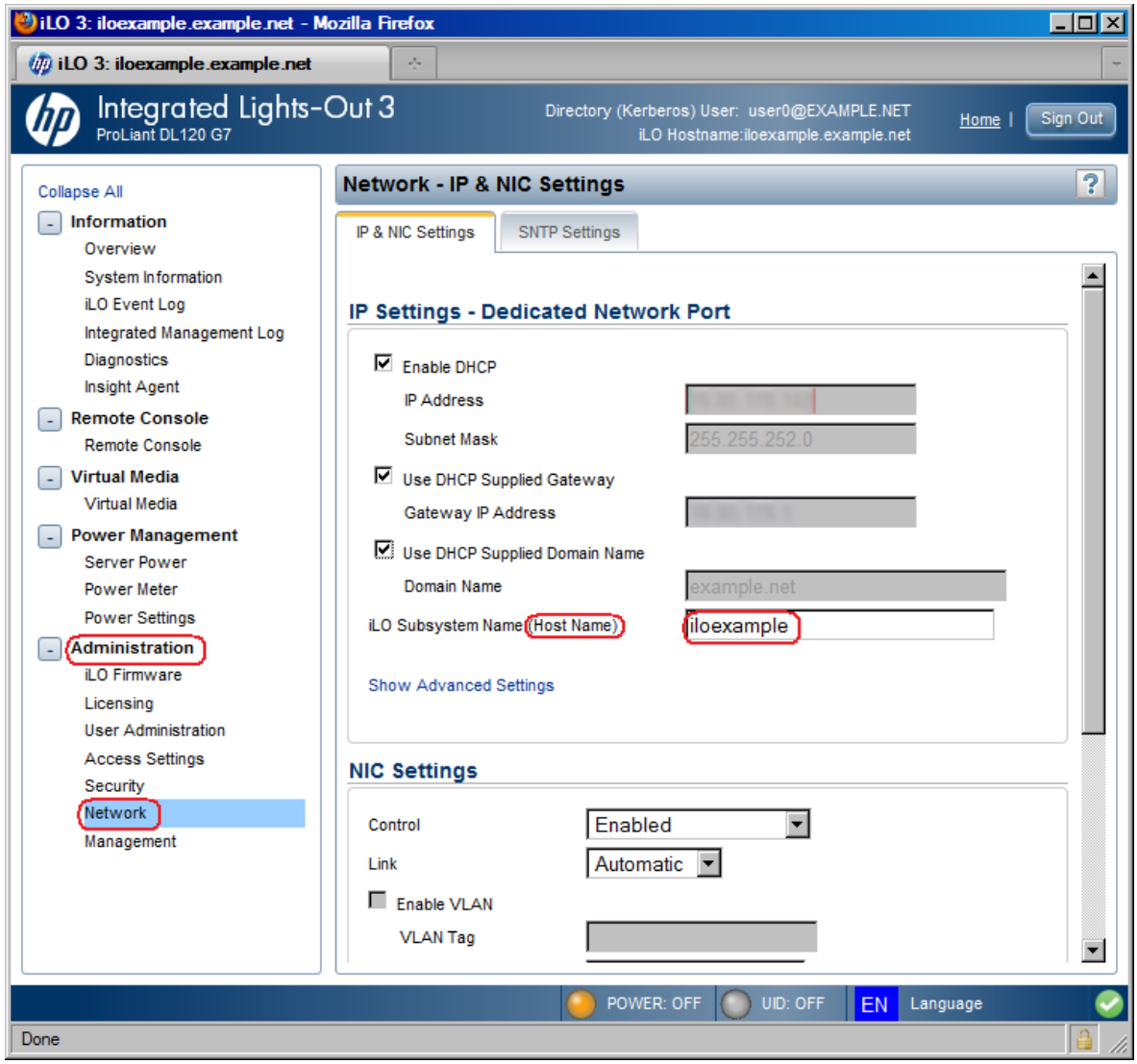
- iLO hostname
- Kerberos authentication enable/disable

- Kerberos realm
- Kerberos KDC **(**Key Distribution Center**)** server address
- Kerberos KDC server port
- Kerberos keytab
- Directory groups
- iLO date/time, SNTP settings

Complete the following steps to use the iLO web interface to set up the Kerberos host name.

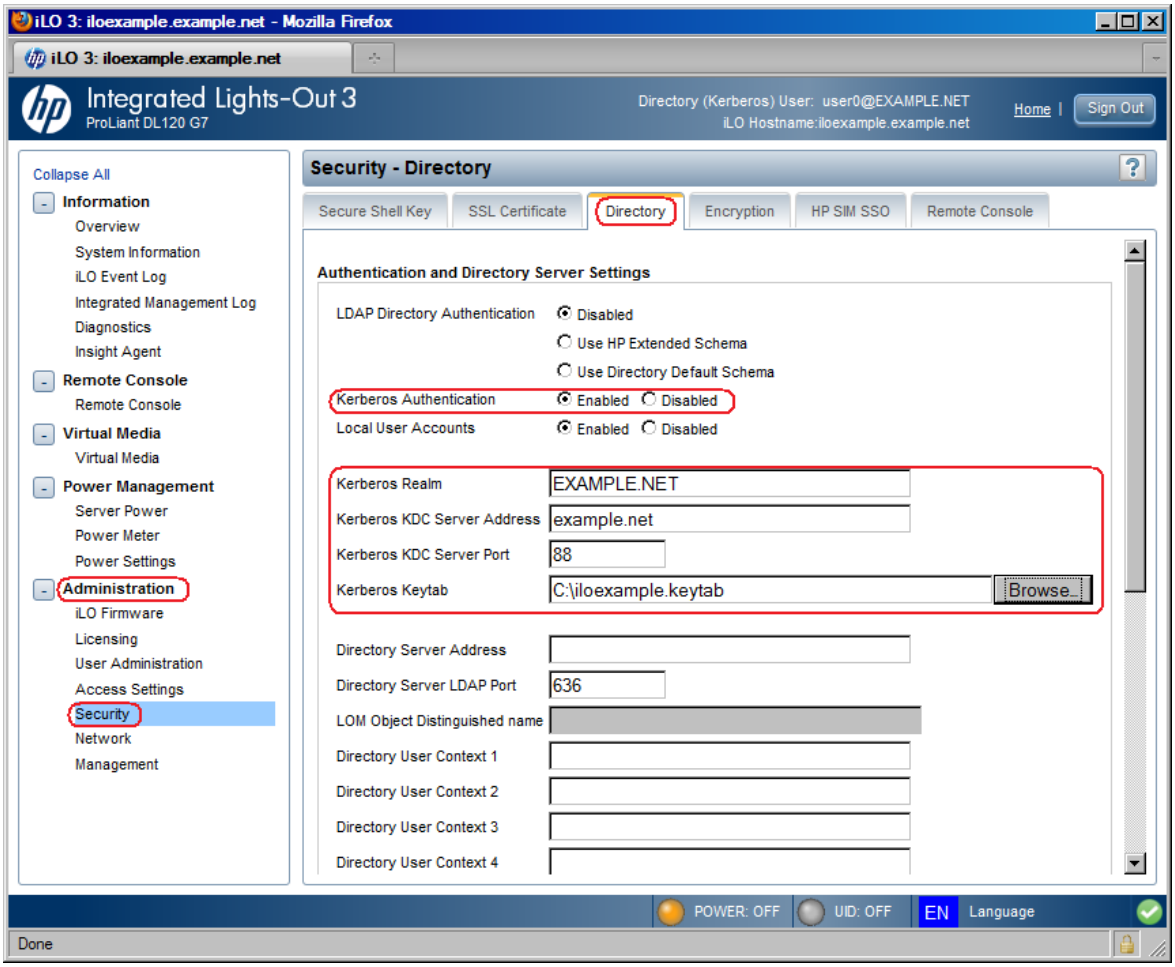
1. Open the iLO web page and click on the Administration tab (Figure 7):
   a. Highlight **Network** in the left pane.
   b. Select the **IP & NIC Settings** tab in the Network – IP & NIC Settings window.
   c. Enter the iLO Subsystem Name (Host Name) in the space provided.

**Figure 7:** Use the iLO web interface to set up the Kerberos host name configuration.



2. In the Security – Directory window, click on **Administration** in the left pane (Figure 8).
   a. Highlight **Security** in the left pane.
   b. Select the **Directory** tab in the Security – Directory window.
   c. Enable the Kerberos Authentication option.
   d. Enter the **Kerberos realm name**, **Kerberos KDC server address**, and **Kerberos KDC server port**. Then browse to and select the binary file containing the **Kerberos keytab.**
   e. Generate your keytab file manually, if necessary. Refer to the next section, "Manually generating a keytab file."

**Figure 8:** Use the Security-Directory window to configure the Kerberos parameter.

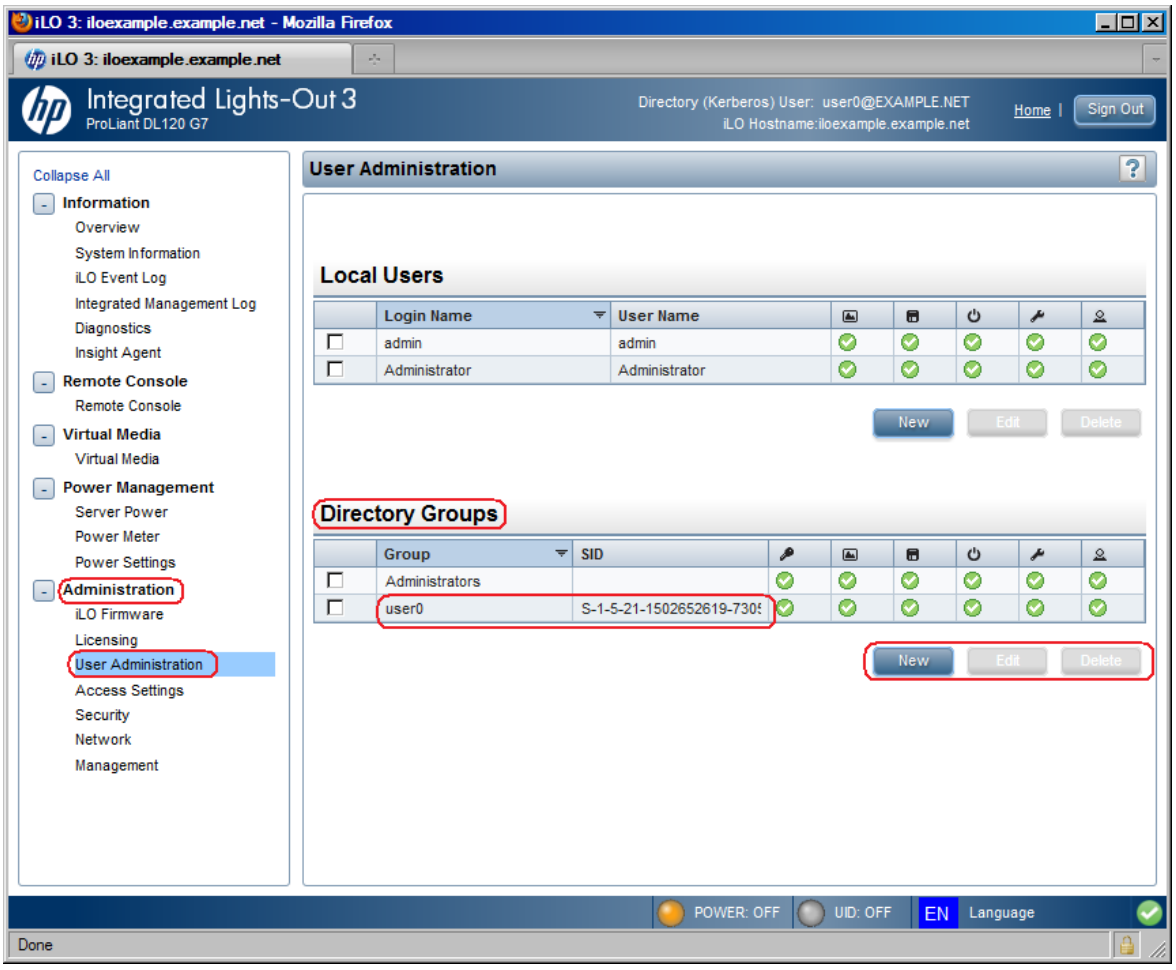


**Note:**
To get the ktpass and SetSPN commands for execution on Windows XP, install the Windows Server 2003 Service Pack 2 support tools, KB926027 or later. Earlier versions will not work.

You can also install KB926027 on Windows Vista, but not all features will work correctly. The ktpass and SetSPN commands will work correctly.

3. Click **Administration** and then **User Administration** in the left pane (Figure 9).
4. Select the Directory Group that you want to modify (user0 in Figure 9). Click **Edit** or **New**. You can use Directory groups to grant permissions to users logging in to iLO.

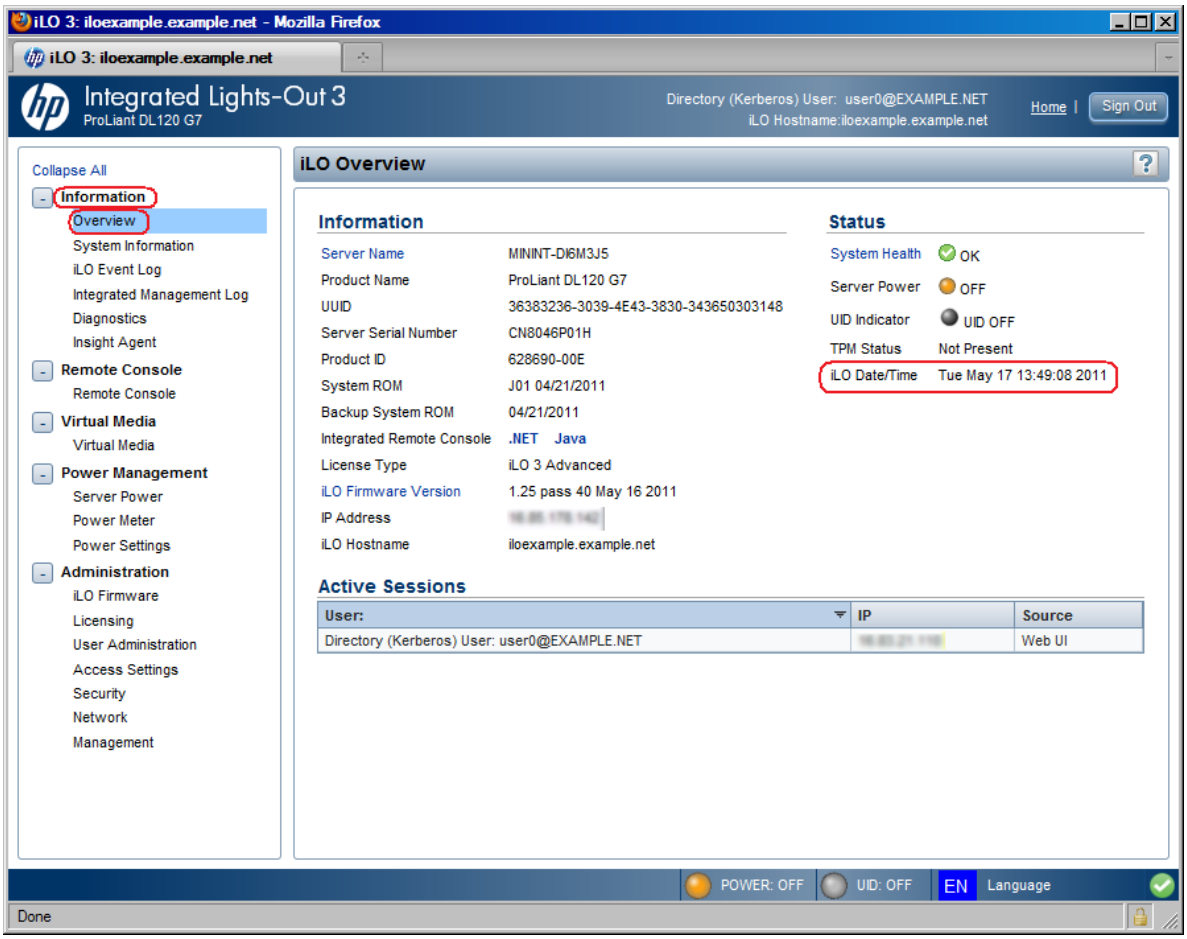
**Figure 9:** Use the User Administration window to configure Directory Groups.




5. Click **Information** and then **Overview** in the left pane (Figure 10).
   Use the iLO Overview window to compare the date and time on the iLO management controller, the KDC, and the client workstation to ensure that the date and time settings on all are synchronized. Kerberos authentication will not function properly if they are not

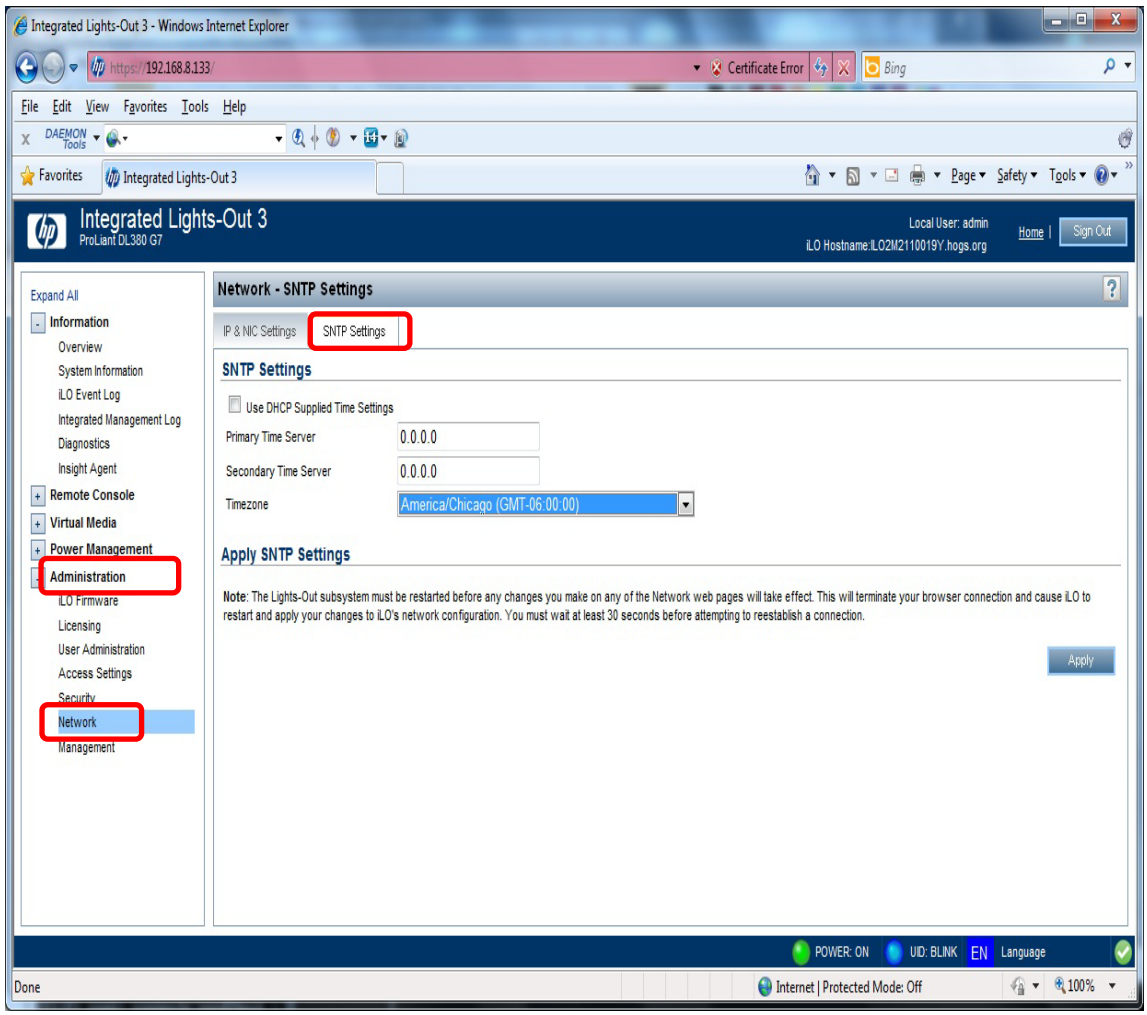
synchronized. Either allow the associated server to set the date/time, or enable the SNTP settings feature within iLO.

**Figure 10:** Use the iLO Overview window to synchronize date and time references.



6. To enable SNTP, select **Administration** > **Network** > **SNTP Settings** (Figure 11).

**Figure 11:** Use the Network – SNTP Settings window to configure SNTP settings.




# Manually generating a keytab file

The example in this section shows how to generate a keytab file for the iLO interface in a Windows environment.

Use the ktpass command to generate a keytab file and set the shared secret. Note that the command is case sensitive and has special characters:

```
ktpass -out iloexample.keytab +rndPass -ptype KRB5_NT_SRV_HST -mapuser
iloexample$@example.net -princ HTTP/iloexample.example.net@EXAMPLE.NET
```

The output should be similar to this:

```
Targeting domain controller: domaincontroller.example.net
Using legacy password setting method
Successfully mapped HTTP/iloexample.example.net to ILOEXAMPLE$.
```

```
WARNING: pType and account type do not match. This might cause
problems.
Key created.
Output keytab to iloexample.keytab:
Keytab version: 0x502
keysize 69 HTTP/iloexample.example.net@EXAMPLE.NET ptype 3 (KRB5
_NT_SRV_HST) vno 3 etype 0x17 (RC4-HMAC) keylength 16
(0x5a5c7c18ae23559acc2
9d95e0524bf23)
```

Note that ktpass may prompt that it is unable to set the UPN. This is acceptable because the iLO interface is a service, and not a user. The ktpass command may also prompt that it is OK to change the password on the object. Ultimately, the system generates the keytab file.

Do **NOT** use the -kvno option with ktpass. That would make the knvo in the keytab file out of sync with the kvno in Active Directory.

Use the SetSPN command to assign the Kerberos SPN to the computer object:

```
SetSPN -A HTTP/iloexample.example.net iloexample
```

If SetSPN gives an error, use MMC with the ADSIEdit snap-in, find the computer object for the iLO, and set the dNSHostName property to the iLO's DNS name. The iLO's DN will be something like this:

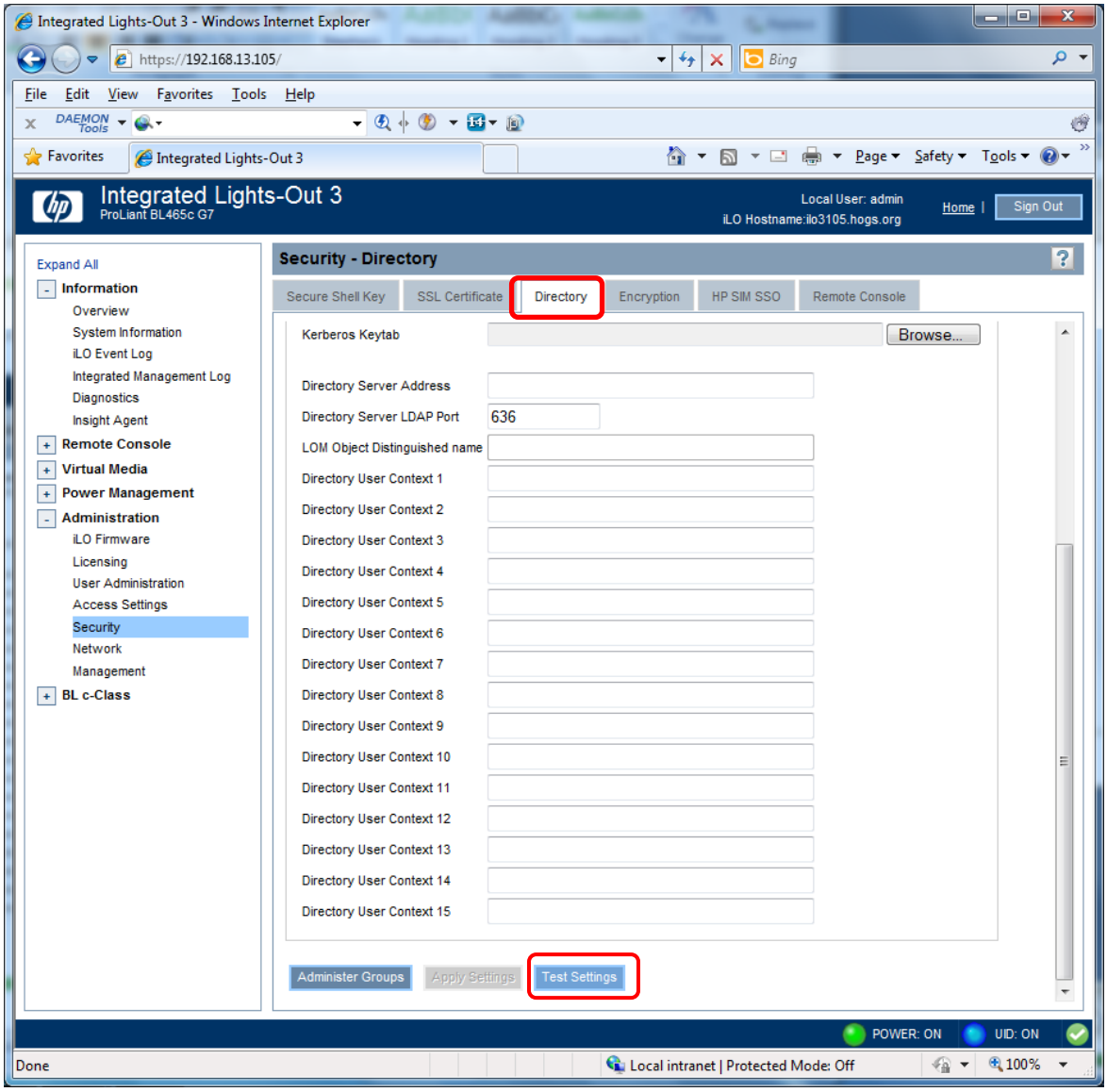
```
cn=iloexample,ou=us,ou=clients,dc=example,dc=net
```

Use command "`SetSPN -L iloexample`" to show the SPNs and DN for the iLO3. Verify that the "`HTTP/iloexample.example.net`" service is listed.

# Validating the directory

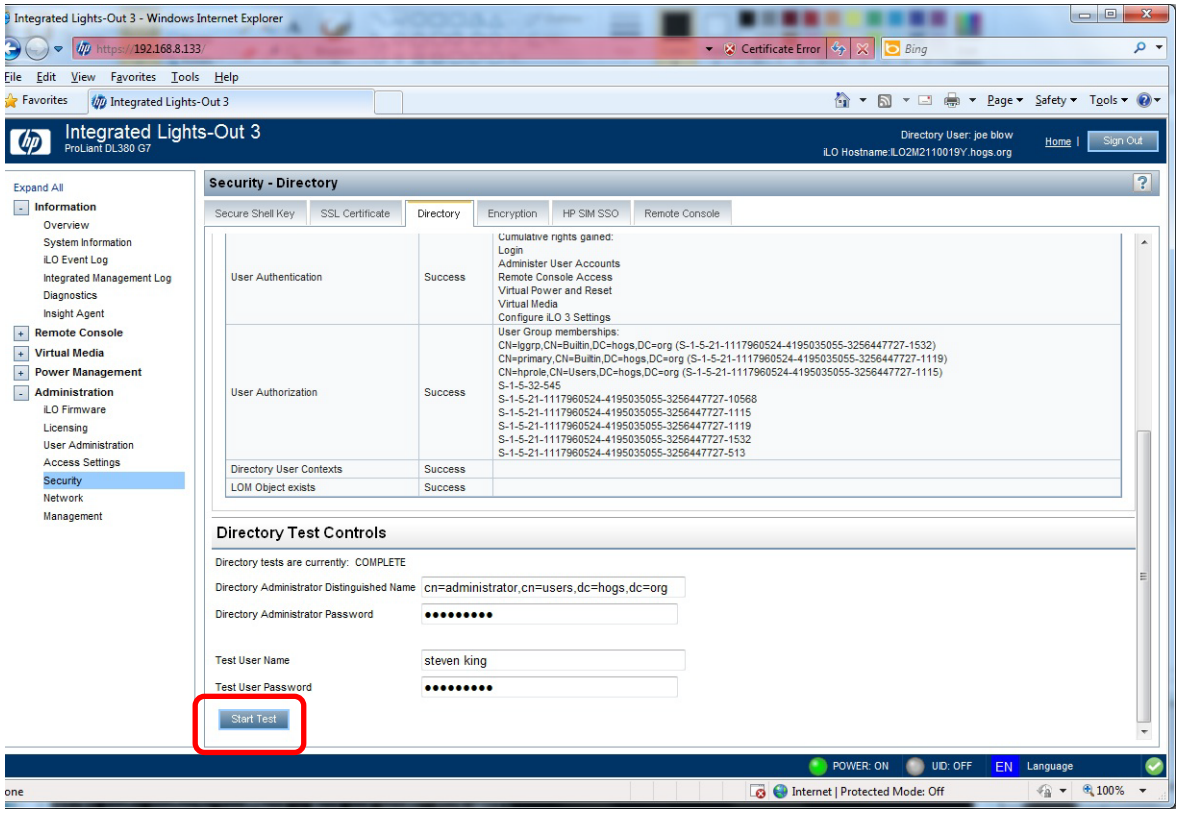
To validate the directory, select the **Directory** tab in the web interface. Then click **Test Settings** (Figure 12).

**Figure 12:** Use the Security – Directory window to validate the Lights-Out directory settings.



When the Directory Tests window appears, click **Start Test** (Figure 13).

**Figure 13:** Click the **Start Test** button to initiate the Directory Tests.

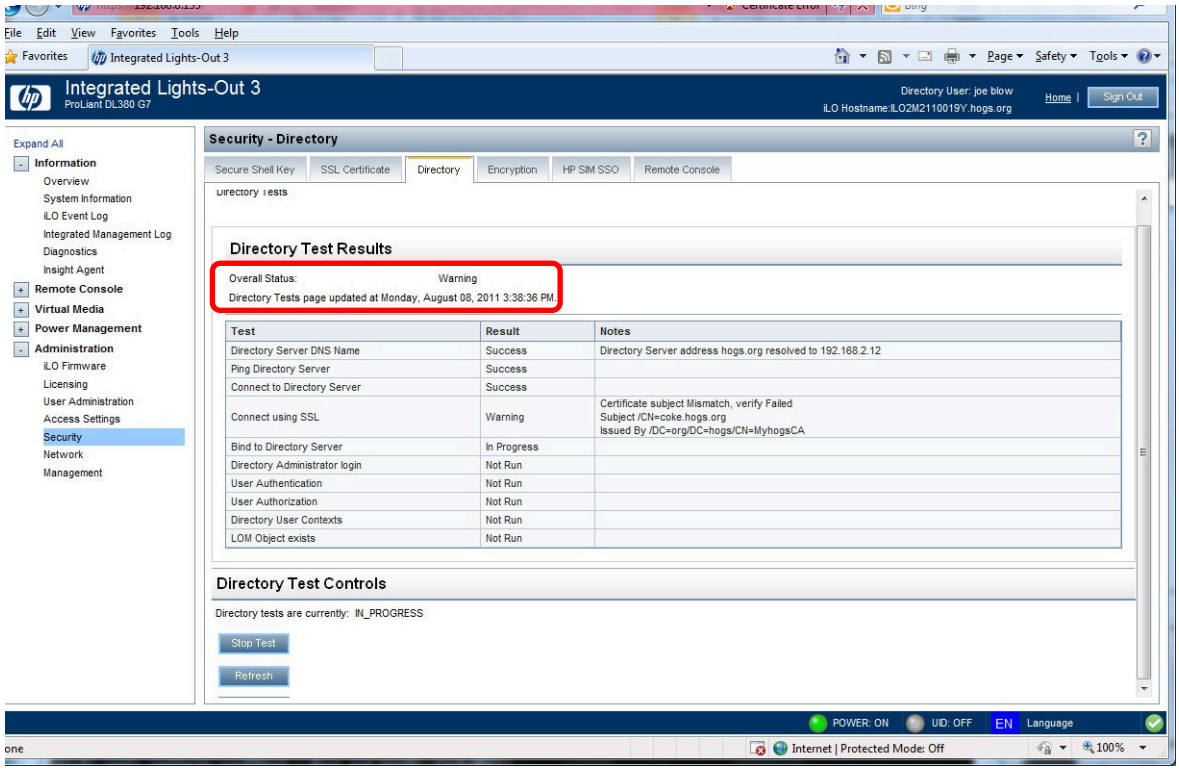


## Test results

The Results screen (Figure 14) reports after the tests complete, after a test fails, or after you cancel the tests. Depending on the test selected, you can see results for specific directory settings or for an operation using one or more directory settings. The directory may not be available if the directory test fails.

The Overall Status line summarizes results of the whole test series.

**Figure 14**: Check the Directory Test Results after the tests complete.

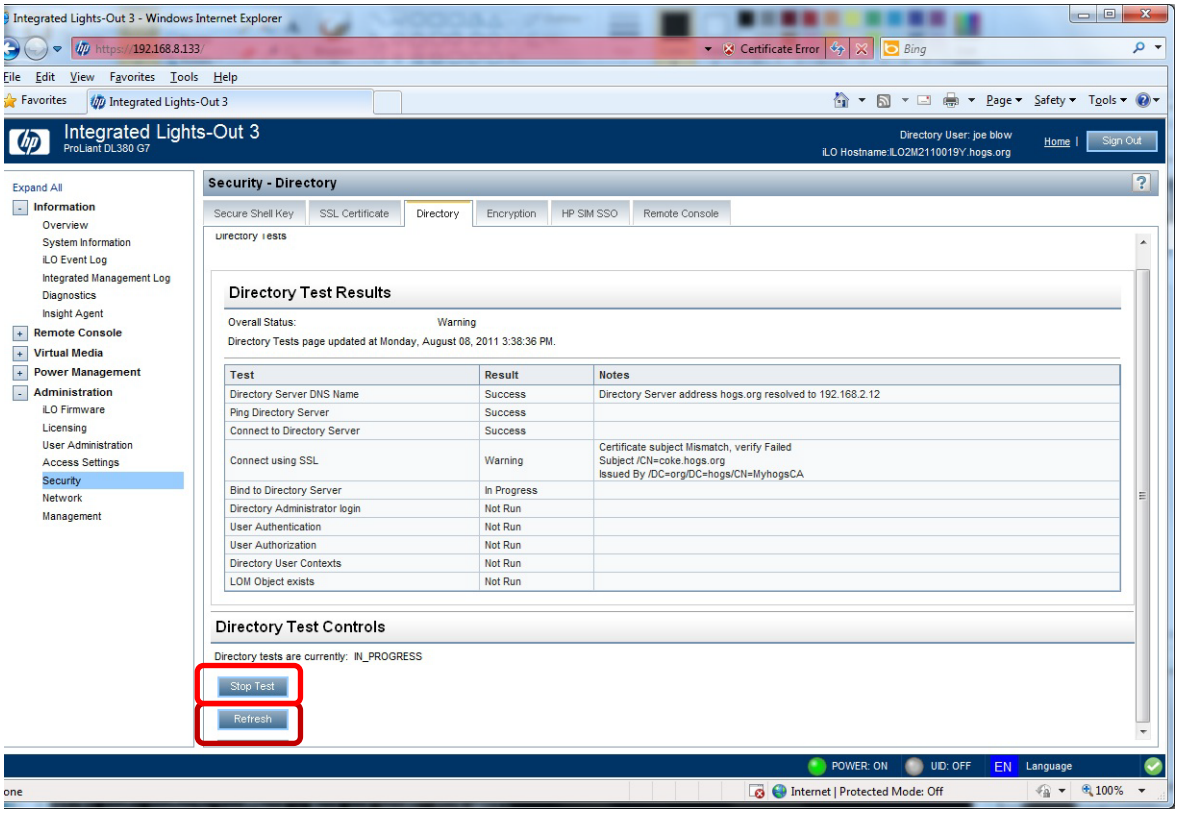


## Canceling tests

Click on the **Stop Test** button (Figure 15) to cancel tests in progress. A test may not stop immediately. Directory tests with **Stopping** in the Result field have not yet reached a point where they can stop.

HPQLOMIG does not update the test results automatically if you cancel a test. Use the **Refresh** button (Figure 15) to check whether the tests have completed or stopped.

**Figure 15**: Cancel tests in progress or use the **Refresh** button to check their status.




## Rerunning tests

You cannot restart tests until the status changes to **Not Running**. Once that happens, enter new parameters to rerun any tests listed as **Not Running**. Then use the **Start Test** button to begin the tests with the new parameters.

Table 1 lists the types of directory tests that you can run, the result when tests are successful, and the result when tests fail.

**Table 1: Directory settings tests and possible results**

| Test name | Successful result | Failed result |
|---|---|---|
| Ping Directory Server | The directory server responds to the ping test. | The iLO processor could not verify a host at the Directory Server Address. |
| Directory Server DNS Name | The directory server address uses the DNS naming format, and iLO successfully searched for a network address using the directory server name. | iLO could not get an IP address for the directory server. Possible reasons:<br>• The Directory Server Name was malformed.<br>• The DNS server did not have an address for the directory server.<br>• The DNS server did not respond.<br>• iLO did not have a proper DNS configuration. |
| Connect to Directory Server | iLO accepted the directory server address and LDAP port. This lets iLO open a network connection to the directory server. | The host server at the Directory Server Address refused a connection on the Directory Server LDAP port or the connection timed out. To troubleshoot, verify that the port number is correct. |
| Connect using SSL | iLO negotiated a secure communication channel with the directory server and completed an SSL handshake. | A failure may indicate that the directory server is not accepting SSL connections. This can occur when the AD server has no SSL Certificate installed (see the "Checking LDAP over SSL" section of this paper). |
| Certificate of Directory Server | iLO received a directory server certificate during the SSL handshake. | The certificate subject did not match the Directory Server Address. This may happen if the certificate was generated using a DNS name and the Directory Server Address is specified in IP notation. |
| Bind to Directory Server | The directory server accepted the credentials. | A failure indicates that iLO rejected the credentials or that the bind operation timed out. Anonymous binds occur when iLO makes a connection with no username. |
| User Authorization | The user can access the iLO processor. | The Test User credentials could not gain any rights to iLO when accessing the directory server. Check the user groups and group membership in the Active Directory Users and Computers Tool. |
| Directory Administrator Login | The directory server authenticated the administrator distinguished name and password.<br>This connection verifies the LOM object settings and user search contexts. Other tests may not run if you did not supply administrator login credentials or the credentials are invalid. | The directory server rejected the credentials. |
| User Authentication | The iLO processor granted access to the user. | The directory server rejected the Test User Name and Test User Password, even when applying search contexts. |

| Test name | Successful result | Failed result |
|---|---|---|
| Directory User Context | The test passes when a user login succeeds using the directory user context. The test also passes when iLO can find the context container object in the directory using the administrator's credentials. You can only test contexts beginning with "@" by user login. | The object could not be located when the iLO used the Directory Administrator credentials to search for the container. iLO 3 v1.0 and greater let you specify up to 15 user contexts. |
| LOM Object Exists | This test does not run with schema-free integration. | |

# Preventing user access issues

Understanding how iLO authorizes users can help you prevent user access issues. iLO performs the following steps to authenticate and authorize an LDAP user with the schema-free method:

1. iLO connects to the configured directory server and passes the user name and credentials. iLO tries to build a better user name if the user name does not authenticate. It uses the search contexts and appends them to get an authenticated connection to the directory server:
   a. For contexts beginning with @, iLO uses "username@context".
   b. For contexts similar to "cn=context", iLO uses "cn=username, cn=context".

   Note that even a user without rights to iLO can get an authenticated connection with the directory server.
2. iLO calculates the user rights from two sources:
   a. iLO reads the authenticated user's MemberOf attribute and compares the listed groups with iLO-configured groups.
   b. iLO also reads each configured group and the group's ObjectSID (security identifier), searches for the user, and then reads the authenticated user's TokenGroups attribute. iLO compares the values to determine if the user is a member.

iLO assigns rights based on the discovered membership.

## Cross-domain considerations

The following situations may cause user access problems across multiple domains:

- If you configure iLO to use the directory server from one domain, users from other domains cannot log in unless the server is running Active Directory Server 2008 and groups have a configured SID.
- If you configure iLO to use the directory server from one domain, groups from other domains will not assign rights unless the user is a direct member of those groups and groups have a configured SID.
- If you configure iLO to use the global catalog, groups that are not replicated to the catalog will not assign rights.

You can replicate and test for the situations above by using an LDAP test tool such as Microsoft ldp.exe.

## User login considerations

The Name field on the iLO login page can accept Directory user names in the following forms:

- LDAP fully distinguished name such as cn=John Smith, cn=Users, dc=MyCompany, dc=COM
- DOMAIN\user name form such as MyCompany\jsmith
- Username@domain form such as jsmith@MyCompany.com
- User name form such as John Smith

You can use a maximum of 1024 characters (1 kilobyte) for the Directory Services/user/names.

Active Directory will accept non-LDAP forms of the user name such as "domain\username" or "username@subdomain.domain." However, iLO cannot use these forms to read the user object. iLO must use search contexts to convert the username to the LDAP form.

You can use iLO Directory User Context fields to pre-define user organizations so users can log in with only their common names. The section "Preventing Lights-Out user access issues" in this paper describes how iLO authenticates users. iLO 3 (v 1.0 and greater) uses the Default Naming Context from the directory server as an additional Directory User Context.

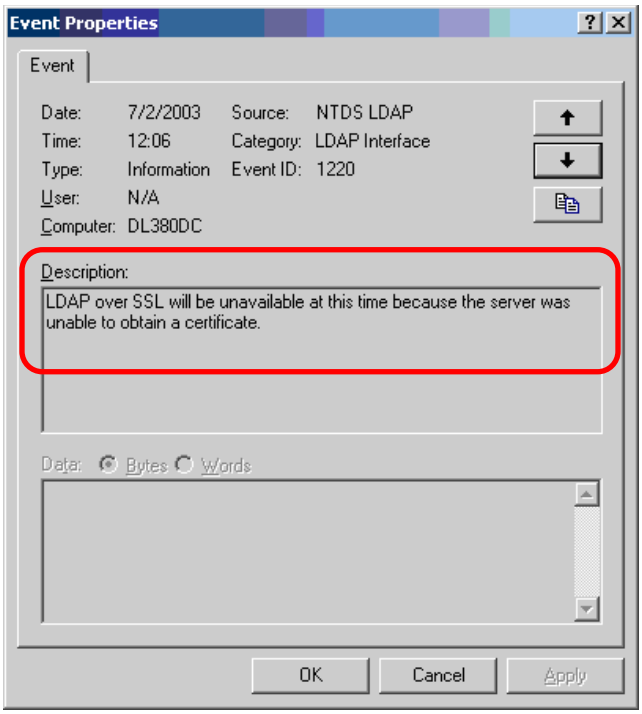
## Checking for LDAP over SSL

For authentication to work correctly between iLO and the domain controller in AD, the domain controller must have LDAP over SSL capabilities. This means the domain controller must have a certificate assigned by a Certificate Authority. See the Microsoft Knowledge Base for more information on installing a Certificate Server on a domain controller so that other domain controllers can automatically obtain certificates.

You can also use existing PKI infrastructure to obtain certificates. For information about this, refer to Microsoft Knowledge Base article at http://support.microsoft.com/kb/321051/

If AD authentication fails, check the event log for an LDAP error, as illustrated in Figure 16.

**Figure 16**: Check the event log for an LDAP error.




## Testing for a non-working SSL

A domain controller with a non-working SSL can cause authentication problems in its domain. Follow these steps to test SSL:

1. To see which domain controller handles requests for the domain, open a browser and navigate to https://<Domain Controller>:636 or to https://<domain>:636.
2. If SSL is operating properly on a domain controller, the Security dialog box will ask if you want to access the site and will offer to view the server certificate. The appearance of the Security dialog box indicates that the server is working.

   If a "page cannot be displayed" message appears instead of the Security dialog box, then the domain controller is not accepting SSL connections. This is most likely because the domain controller doesn't have a certificate.

   If auto-enrollment is enabled, the domain controller issues and installs certificates automatically, but a reboot may be required. To avoid a possible reboot and to force issuing a certificate, perform the following additional steps:
3. Open Microsoft Management Console (MMC) and add the **Certificates** snap-in.
4. When prompted, select **Computer Account** for the type of certificates you want to view. Click **OK** to continue, and return to the Certificates snap-in.
5. Right-click on the **Personal/Certificates** folder. On the right, click **More Actions**, and then **All Tasks > Request New Certificate**.
6. Click **Next**, select **Domain Controller**, and then click **Enroll**.

For an alternate method to check SSL, use the Microsoft ldp.exe tool.

**NOTE:**

It may be useful to test multiple domain controllers for issuing a certificate. iLO can use a backup domain controller if the primary domain controller is unavailable.

## Removing/replacing old certificates

An old certificate on a domain controller may point to a previously trusted Certificate of Authority (CA) with the same name. This usually does not happen unless you have added, removed, and then added Certificate Services again on the domain controller. See the previous section ("Testing for a non-working SSL") to check and re-issue a certificate.

For more information about old certificates, refer to HP Customer Advisory EM030604 CW01S available at http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=PSD_EM030604_CW01&locale=en_U.

# Configuring the Kerberos client with Internet Explorer

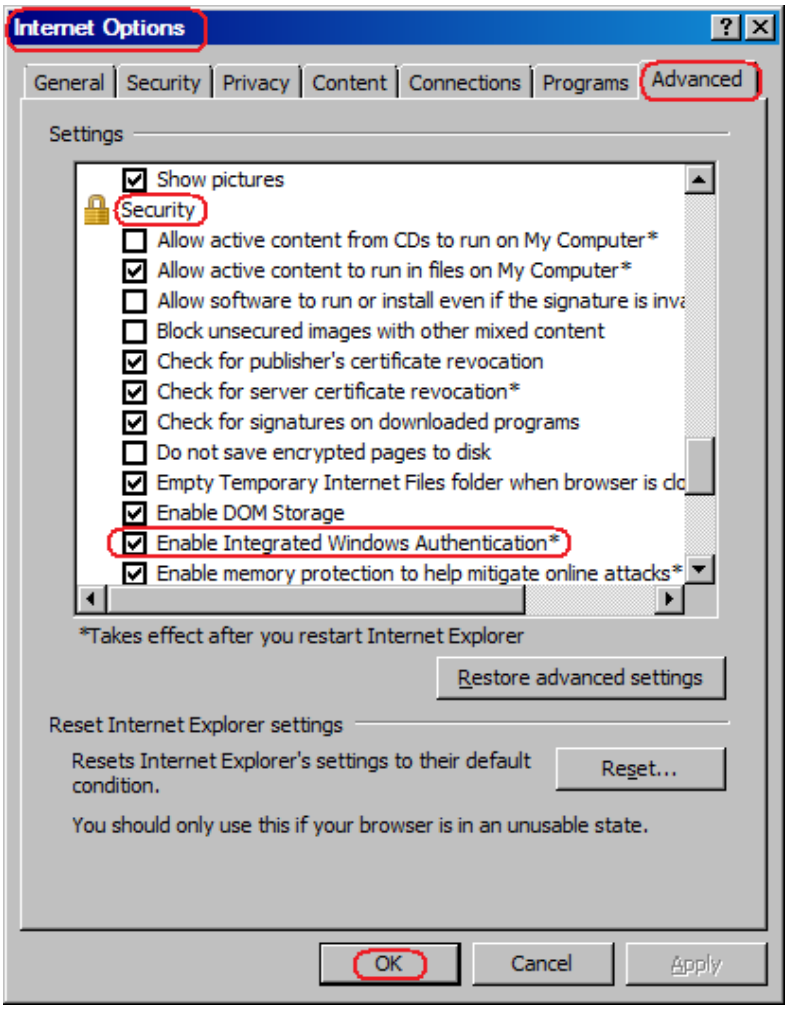
To log into iLO, you must be a member of a group with assigned permissions. For Windows clients, locking and unlocking the workstation will refresh the login credentials for iLO. Home versions of Windows operating systems do not support Kerberos.

To enable single sign-on with Internet Explorer (IE), complete the sequence of steps in the following sections.

## Enabling authentication in Internet Explorer

1. From your Home page, select **Tools > Internet Options** (Figure17).
2. Select the **Advanced** tab.
3. Scroll to **Security**.
4. Verify that **Enable Integrated Windows Authentication** is checked.
5. Click **OK**.

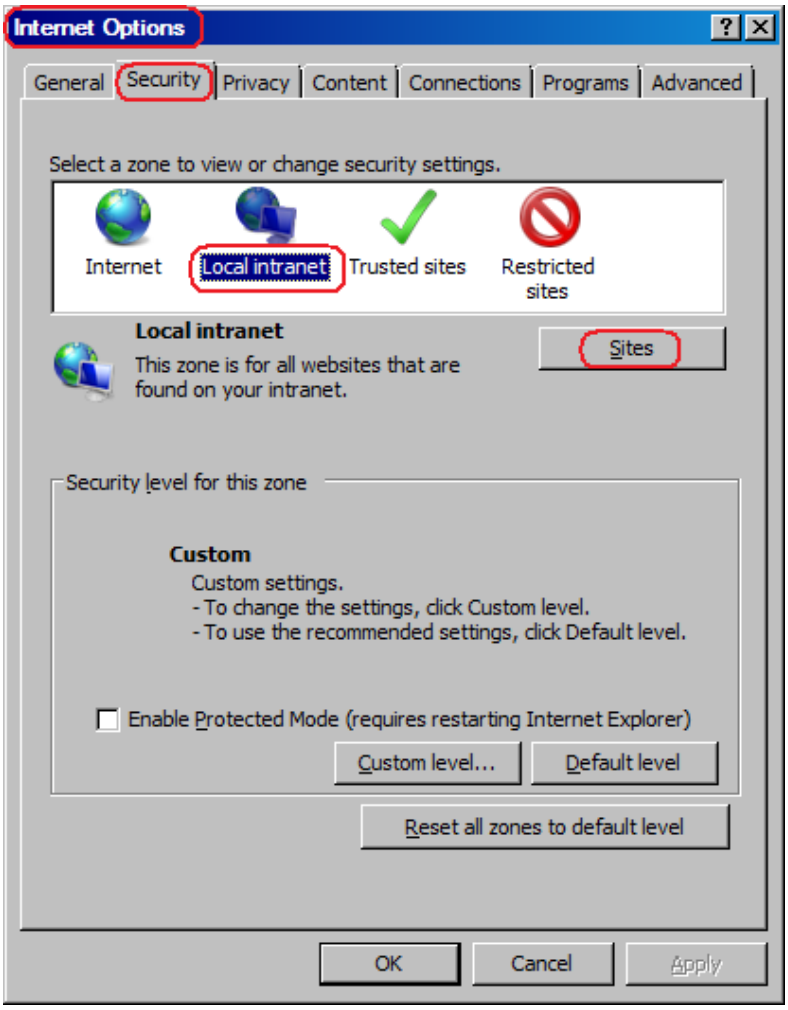
**Figure 17:** Enable integrated Windows authentication in Internet Explorer.



## Verifying that the iLO domain is in the Intranet zone

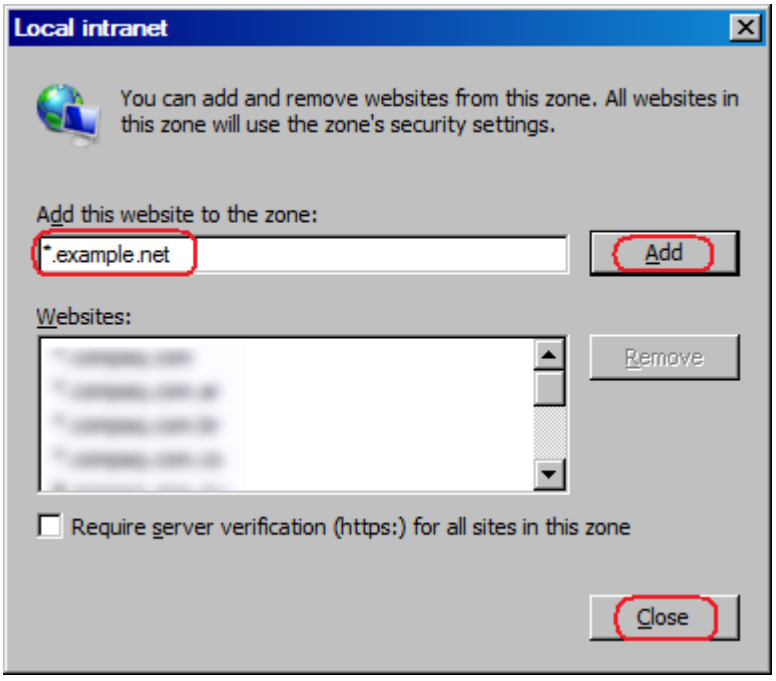
1. From your Home page, select **Tools > Internet Options**.
2. Select the **Security** tab (Figure 18).
3. Click the **Local Intranet** icon, and then click the **Sites** button.

**Figure 18:** Configure local Intranet sites in Internet Explorer.



4. Click the **Advanced** button.
5. Enter the website name in the text box provided (Figure 19).

**Figure 19:** Add website to the zone.

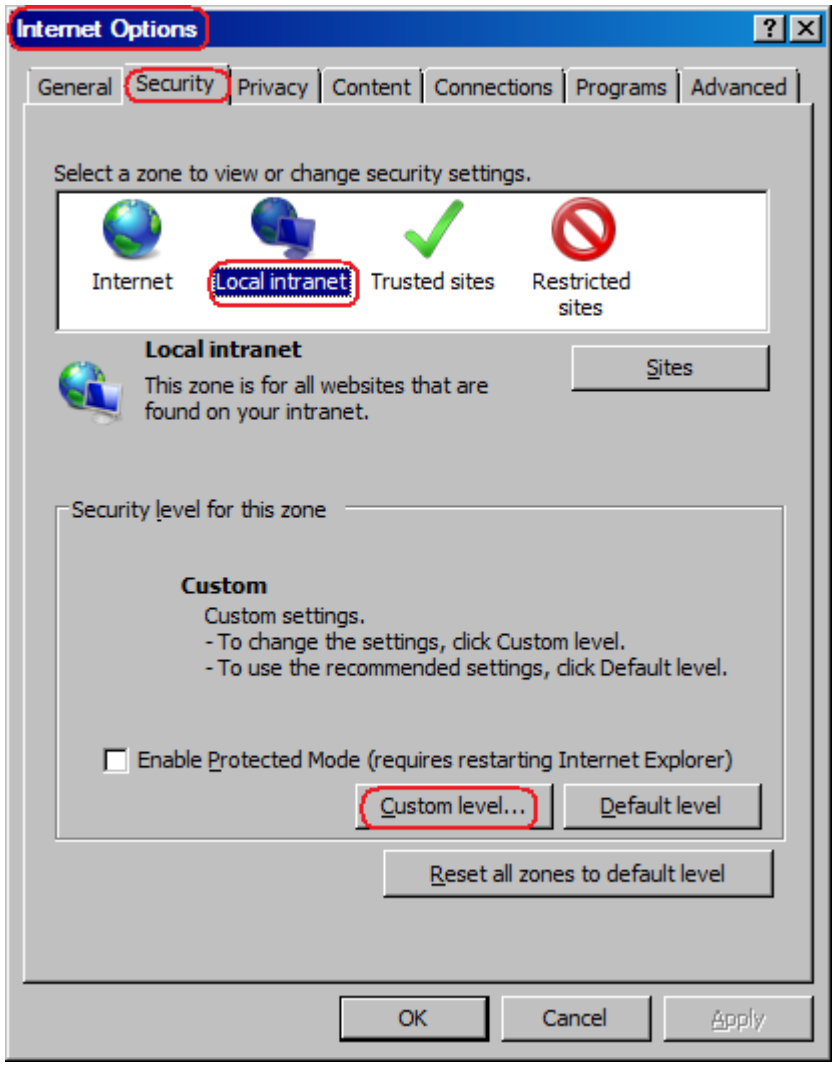



6. Click **Add** and then **Close**.
7. Click **OK**.
8. Click **OK**.

## Setting custom security levels

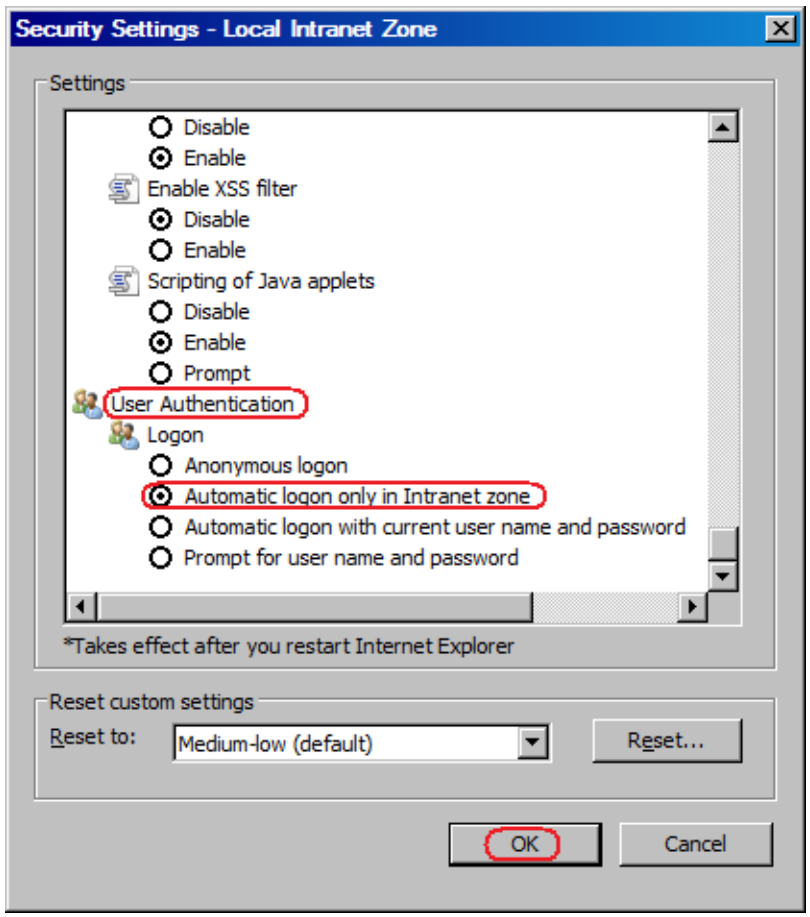
1. From your Home page, select **Tools > Internet Options**.
2. Select the **Security** tab (Figure 20).
3. Click the **Local Intranet** icon, and then click the **Custom level…** button.

**Figure 20:** Configure custom security levels in Internet Explorer.



4. Scroll to **User Authentication** (Figure 21).

**Figure 21:** Verify User Authentication in Internet Explorer.




5. Select **Automatic logon only in Intranet zone**.
6. Click **OK**.
7. Click **OK**.
8. If you changed any of the options, close and restart Internet Explorer.
9. Once you restart Internet Explorer, use the fully qualified domain name to browse to the iLO interface and sign in.
10. Click the **HP Zero Sign In** button (Figure 22) to logon to iLO.

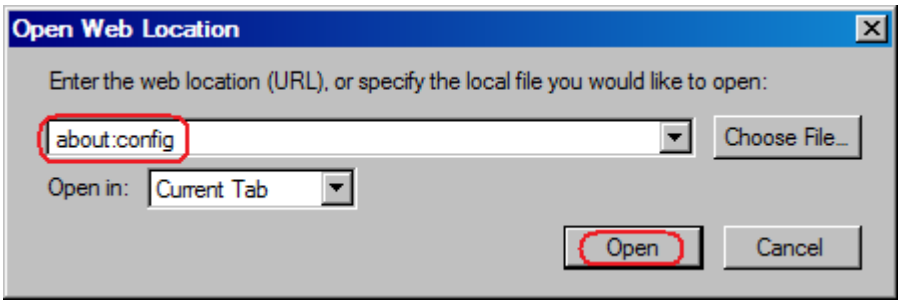
**Figure 22:** Click the **HP Zero Sign In** button to logon to iLO.

# Configuring the Kerberos client with Firefox

To enable single sign-on with Firefox, complete the following sequence of steps. Setup for Firefox 3.5 and for Firefox 3.6 is similar.

1. To open the browser configuration page, enter **about:config** in the space provided (Figure 23), and click the **Open** button.

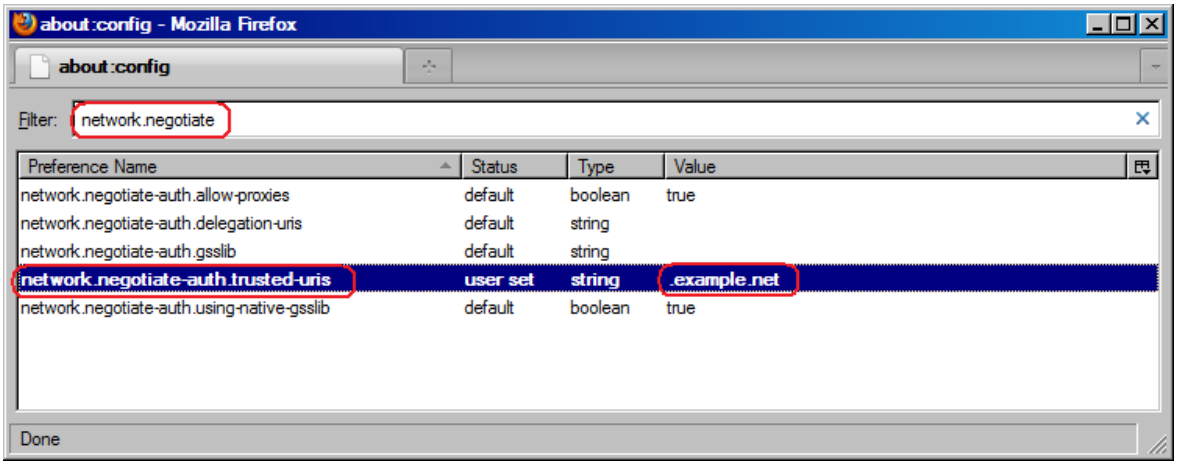
**Figure 23:** Open the browser configuration page.




If the message "This might void your warranty!" appears, click the **I'll be careful, I promise!** button.

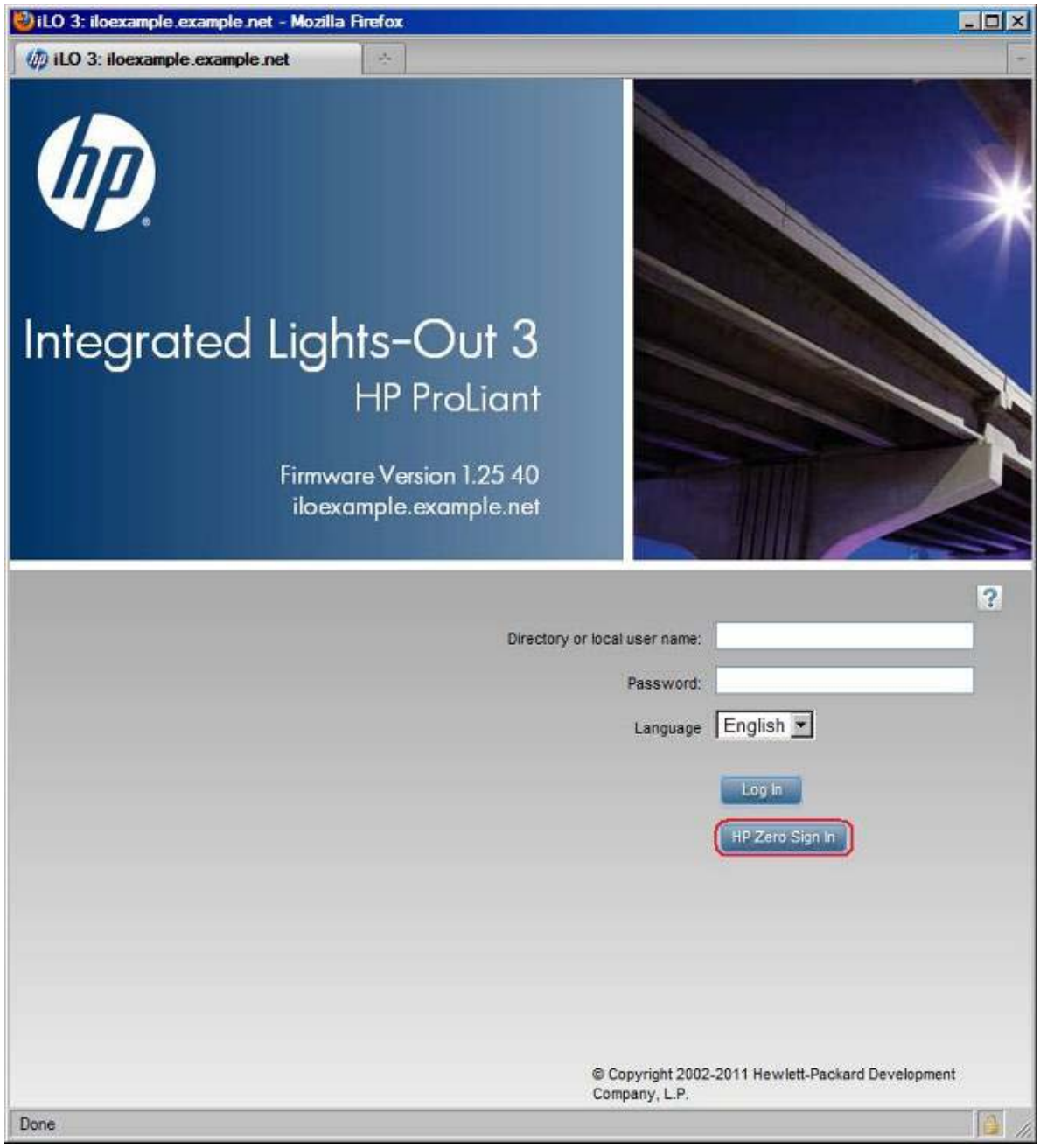
2. In the Filter field, enter network.negotiate (Figure 24).
3. Double-click **network.negotiate-auth.trusted-uris** to modify the value.
4. Enter the DNS name for the iLO ("ilo.example.net").

**Figure 24**: Configure trusted URLs in Firefox.



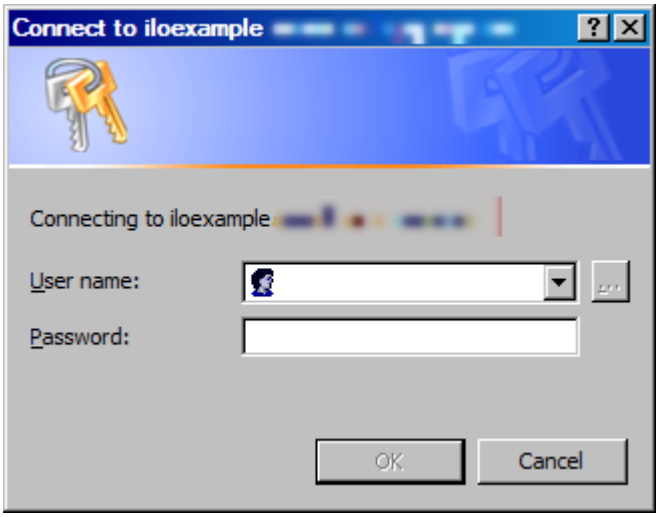
5. Browse to the iLO interface using the fully qualified domain name.
6. Browse to the iLO login page, and click the **HP Zero Sign In** button (Figure 25).

**Figure 25:** Click the **HP Zero Sign In** button to logon to iLO.



If a prompt for credentials appears (Figure 26), Kerberos authentication failed and the system fell back to NTLM (Windows NT LAN manager) authentication instead.

**Figure 26**: If the Credentials prompt appears, Kerberos authentication failed.




Browse to the iLO login page, and log in by name. Use the username in the Kerberos SPN form and the associated domain password.

# Conclusion

Increasingly, enterprise customers are using directory services to address security and to reduce management costs. Using your existing Microsoft Active Directory, you can authenticate access and authorize user privileges to iLO management devices. This integration with directory services improves efficiency by letting you configure and maintain the user accounts for the iLO devices in a central, scalable database.

# For more information

Visit the URLs listed below if you need additional information.

| Resource description | Web address |
|---|---|
| Integrated Lights-Out products | www.hp.com/go/iLO |
| "Integrated Lights-Out Technology: Enhancing the Manageability of ProLiant Servers" technology brief | http://h20000.www2.hp.com/bc/docs/support/SupportManual/c00257345/c00257345.pdf |
| HP ProLiant servers and solutions | www.hp.com/servers/proliant |

Send comments about this paper to TechCom@HP.com

 Follow us on Twitter: http://twitter.com/ISSGeekatHP



TC0000804, September 2011